

**IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
at CHATTANOOGA**

IN RE: SEARCH OF THE RESIDENCE)	
AND CURTILAGE LOCATED AT)	MAGISTRATE NO:
839 15TH STREET, NORTHEAST,)	
CLEVELAND, TENNESSEE 37311)	UNDER SEAL
WHICH IS MORE PARTICULARLY)	
DESCRIBED IN ATTACHMENT B1)	
AND B2)	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jeremy P. Allman, Affiant, being first duly sworn, depose and state as follows:

1. I am a Crimes Against Children Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), currently assigned to the Knoxville Division, Chattanooga, Tennessee Resident Agency. I have been a law enforcement officer in the State of Tennessee for approximately twelve years and I am currently a detective with the Bradley County Sheriff's Office. I have investigated criminal violations related to crimes against children and cyber-crime. I have received formal training and have participated in search warrants in a variety of investigative matters. As a task force officer, I am authorized to investigate violations of laws of the United States, and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

2. This application is based, in part, upon information and evidence gathered during an ongoing investigation being conducted by the Federal Bureau of Investigation. The facts set forth in this affidavit are based on that investigation including information provided by other law

enforcement officers, my own personal observations and knowledge, review of documents, review of computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and the training and experience of others.

3. This affidavit is being submitted in support of an application for a search warrant to search the following premises, curtilage, outbuildings, and vehicle(s): 839 15th Street Northeast, Cleveland, Tennessee 37311 (hereinafter "Subject Premises"), which is more fully described as a residential home in Attachment B1 and B2 of this affidavit, which includes a photograph of the residence. This residence is located in Bradley County, which is in the Eastern District of Tennessee.

4. The purpose of this application is to seize evidence of violations of Title 18, United States Code §§ 2252A(a)(1) (any person knowingly transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography), §§ 2252A(a)(2) (any person knowingly receives or distributes any child pornography or material that contains child pornography), §§ 2252A(b)(1) (attempts or conspires to receive, distributes, or transports child pornography), and/or §§ 2252A(a)(5)(B) (any person who knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using

materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including a computer).

5. This affidavit will show there is probable cause to believe that evidence, including records, fruits, instrumentalities, and other items related to the violations being investigated (as specifically described in Attachment A, attached hereto and incorporated herein) will be found at 839 15th Street Northeast, Cleveland, Tennessee 37311, the Subject Premises. Affiant believes two brothers, Larry Oliver and Kenneth Ray Oliver, occupy the Subject Premises. As is more fully described below, the IP address assigned to the Subject Premises is registered to Larry Oliver. Kenneth Ray Oliver, the other occupant, is a convicted sex offender. On January 7, 2015, Affiant received information from Detective (Det.) Shaunda Efaw of the Bradley County Sheriff's Office relating to Kenneth Ray Oliver's sex offender registration. That is, that Kenneth Ray Oliver complied with his quarterly reporting on December 10, 2014, and confirmed he lives at 839 15th Street Northeast, Cleveland, Tennessee 37311. Affiant is unaware of how many electronic devices are within Subject Premises and is unaware of which device contains child pornography but maintains there is probable cause to search each device located within the premises, the curtilage or within any vehicle within the curtilage.

6. Because this affidavit is being submitted for the limited purposes of establishing probable cause, I have not included every detail of every aspect of the investigation for this portion of the affidavit. Rather, I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code §§ 2252A(a)(1), 2252A(a)(2), 2252A(b)(1), and/or 2252A(a)(5)(B) are located at the Subject Premises.

APPLICABLE LAW

7. This investigation concerns alleged violations of Title 18, U.S.C., §§ 2252A(a)(1), 2252A(a)(2), 2252A(b)(1), and/or 2252A(a)(5)(B) relating to material involving the sexual exploitation of minors and enticement:

a. 18 U.S.C. § 2252A(a)(1) prohibits any person who knowingly mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography.

b. 18 U.S.C. § 2252A(a)(2) prohibits any person who knowingly receives or distributes any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer; or any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

c. 18 U.S.C. §§ 2252A(a)(5)(B) prohibits any person who knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including computer.

DEFINITIONS RELATED TO CHILD PORNOGRAPHY

8. “Child Pornography” includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. §§ 2256(8).
9. “Visual depictions” include, but are not limited to, undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. §§ 2256(5).
10. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
11. “Minor” means any person under the age of eighteen years. See 18 U.S.C. §§ 2256(1).
12. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, genital-anal, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. §§ 2256(2).

DEFINITIONS RELATED TO COMPUTERS AND THE INTERNET

13. Based upon Affiant's knowledge, training and experience, and the experience and training of other law enforcement personnel who provided me verifiable information, Affiant knows the following:

a) Personal Computer/ "PC": A personal computer or "PC" has become a generic term that refers to a collection of electronic sub-components, usually consisting of a central processing unit; internal memory; various input/output devices, including a display screen, keyboard, mouse, modem, and printer; and internal/external storage devices (discussed below). Affiant states that a personal computer is a natural repository for information and collections, and organization of materials for personal, business, and financial use. Affiant states that the varying unlimited uses of a personal computer make it probable that evidence of dominion, ownership and control of the personal computer and files thereon may be found in varying electronic forms.

b) Computer Storage Media/Devices: A personal computer usually contains one or more of the following electronic storage media/devices: 1) A "hard drive" which allows users to read from and write to a sealed "hard disk." 2) A "floppy drive" that allows users to read from and write to removable "floppy disks". 3)"Compact Disk (CD) Drive" or "Digital Video Disk (DVD) Drive" which allows users to read from and write to super high capacity CD's and DVD's. 4) A "Tape Drive" which allows users to read from and write to cassette style tapes. 5) Various other storage media such as "zip drives", "jazz drives" etc. manufactured for the purpose of storing quantities of data in a removable/transportable format. The personal computer uses the permanently installed hard disk, removable floppy disks, CD's; DVD's jazz/zips etc. to store and retrieve digital information. The disks can contain information critical to the successful

start-up and operation of the computer, as well as information defined by and purposely placed by the computer user. Additionally, the disks can contain information that the personal computer places on it transparent to and unbeknownst to the end user that signifies or reveals events that have occurred while the user was using the personal computer. Due to the nature of digital data, information that a computer user deletes from his/her computer system can remain on the disk indefinitely, and can be recovered and analyzed as easily as existing undeleted information on the disk. In every instance known to Affiant, computers contain components that were manufactured outside of the state of Tennessee and, if found in Tennessee, necessarily contain components that have traveled in interstate commerce.

c) Computer Files: Computer files are delineated collections of computer information. These files allow users to collect, organize and store information in meaningful ways on the computer's storage disks. The magnetic disks referred to above contain files with information critical to the successful start-up and operation of the computer, as well as files defined, created and manipulated by the computer user

d) Computer Graphic Files: Computer graphic files were photographs that have been digitized into computer binary format, or were photographs taken with a “digital” film-less camera that instantly creates the image in computer binary format. Once in this format the graphic file can be viewed, copied, transmitted, and/or printed. Computer graphic files are differentiated by the type of format convention by which they were created. Two common types of computer graphic files encountered are those in JPEG (Joint Photographic Electronics Group) format having the “jpg” file extension, and the GIF (Graphic Interchange Format) format having the “gif” file extension. In addition, there are two primary video graphic files, which can display motion picture graphics. The formats often encountered are in AVI (Audio Visual Interleaved)

format having the "AVI" file extension, and MPEG (Motion Picture Experts Group) format having the "MPG" file extension. There are also other formats. Because the images in this investigation were uploaded using accounts associated with Google, which maintains servers out of the state of Tennessee, Affiant believes the images of child pornography traveled in interstate commerce.

e) The Internet: World Wide Web, USENET, IRC: The Internet is a worldwide computer network which connects computers and allows communications and the transfer of data and information based on a common addressing system and communications protocol called TCP/IP (Transmission Control Protocol/Internet Protocol) across county, state and national boundaries. The Internet is comprised of three distinct areas: First, the World Wide Web (WWW) is a sub-component of the Internet that allows users to access information on remote "server" computers via the HTTP (Hypertext Transfer Protocol) protocol. Second, the Internet is also comprised of a network of Usenet servers that allow users to post E-mail (discussed below) information in pre-arranged topics. Third, the Internet is comprised of a network of "IRC" servers (discussed below) that allow real-time communication between simultaneous users.

f) Internet Service Provider ("ISP"): Individuals who have access to the Internet must have a subscription to, membership in, or affiliation with, an organization or commercial service, which provides access to the Internet computer network. A provider of Internet access is referred to as an INTERNET SERVICE PROVIDER or ISP. An ISP provides users with a dial-up telephone number, high speed connection (or some other form of connection) so users can connect directly to the ISP's computers, which are in turn connected to the Internet.

g) ISP based e-mail: In addition to access to the Internet, ISP's provide users with an Internet e-mail address as part of the subscription benefits for the service. A particular user's

E-mail address is bisected by the “at” symbol “@”, where the information after the symbol indicates the identity of the ISP, and the information before the symbol indicates the identity of the particular user.

h) Web based e-mail: Many entities on the World Wide Web offer free e-mail services to Internet users (e.g. “Yahoo”, “Hotmail”) that require users to return to the entities site to send/retrieve e-mail. A particular user’s Web based E-mail address is bisected by the “at” symbol “@”, where the information after the symbol indicates the identity of the entity providing the service, and the information before the symbol indicates the identity of the particular user.

i) Electronic Mail (“E-mail”): Individuals that utilize the Internet can communicate by using electronic mail (hereinafter referred to as “E-mail”). E-mail is an electronic form of communication, which can contain letter type correspondence and graphic images. E-mail is similar to conventional paper type mail in that it is addressed from one individual to another and is usually private. E-mail usually contains a message header, which gives information about the individual that originated a particular message or graphic, and importantly, the “Internet Protocol” (IP) address, which refers to the origin of the message despite efforts to conceal the origin. ISP based E-mail is usually retrieved from a remote provider and brought local to the user’s computer for the user to open, read, and respond to the e-mail if necessary. Although web based email is usually retained by the remote provider and not purposefully stored local, the personal computer where the e-mail was retrieved may nonetheless contain the e-mail in temporary files. Thus, e-mail transmissions (sent and received) will routinely be found on the user’s fixed hard disk inside the computer

j) Internet Browser “Bookmarks”/ Internet “Favorites”: The ability to view Internet content and specifically HTML protocol is made possible by interpretive software called an

Internet “browser”. Browsers allow users to set up “bookmarks” or “favorites” that create shortcuts to Internet information, particularly useful if the user intends to visit and/or retrieve information from the source on a regular basis. Additionally, the Internet browser software stores information on recent activity on the Internet.

k) Internet Protocol (IP) Address is a unique identifying number specifically assigned to a computer or device that is using the internet. Every machine on the internet has a unique identifying number, called IP Address. The IP can operate with a 32-bit binary number that uniquely identifies a host connected to the internet or to other internet hosts. An IP address is expressed in “dotted quad” format consisting of decimal values of its four bytes separated with periods, e.g. 127.0.0.1. This system allows over 4 billion unique values. This system is also known as IPV4. Each number can only be used by one computer or machine over the Internet at a time.

l) SHA1 Hash: The SHA hash function was designed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) and published by the NIST (National Institute of Standards and Technology) as a U.S. Federal Information Processing Standard. Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States Federal government for use by all non-military government agencies and by government contractors. “SHA” stands for Secure Hash Algorithm. The SHA1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest (digital fingerprint), or to find two different messages which produce the same message digest as referenced in the Federal Information Processing Standards Publication 180-1.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

14. Based upon my training and the experience and training of other law enforcement officers with whom I have had discussions, computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Affiant knows all of the below-described information as the result of his training and experience in the investigation of computer-related crime and by conferring with other law enforcement personnel who investigate computer related crime.

15. Affiant knows that, computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It also has revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

16. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in

connection with child pornography. These are production, communication, distribution, and storage.

17. Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred, or printed directly from the computer. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow as have been the case in the past.

18. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer also has changed that. A device known as a modem allows any computer to connect to another computer through the use of telephone and/or cable lines. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host computers are sometimes operated by commercial concerns, such as AT&T Internet Services and Charter, which allow subscribers to connect to a network, which is in turn connected to their host systems. These service providers allow electronic mail (email) service between subscribers and

sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web; hence they are commonly described as Internet Service Providers (ISPs). Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of “chat rooms” and/or instant messaging. Many ISPs today offer high-speed broadband internet service. Broadband is often called high-speed Internet, because it usually has a high rate of data transmission much higher than the dial-up structure of the past.

19. These communication structures are ideal for individuals who possess, receive and distribute child pornography. The open and anonymous communication allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send text messages and graphic images to other individuals interested in child pornography. Moreover, the child pornographer need not use the large service providers. Child pornographers can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornographers.

20. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred via electronic mail to anyone with access to an electronic device with internet access such as a

smartphone or computer. Because of the proliferation of commercial services that provide electronic mail service, chat services, peer-to-peer services and easy access to the Internet, the computer is a preferred method of receipt and distribution of child pornographic materials.

21. The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of five hundred (500) gigabytes are not uncommon. These drives can store tens of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, save the image, and store it at another location. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

22. Based on Affiant's knowledge, training and experience and training and experience of other officers, child pornographers commonly download and save some of their collection of child pornography from their computer to removable media such as thumb drives, CD-ROMs, and floppy disks so the images can be maintained and mobile and will be easily accessible to the individual. It is not uncommon for the child pornographer to print pictures of child pornography and to keep them in a safe and secure location for easy viewing. Thumb drives, CD-ROMs, floppy disks and external hard drives containing child pornography and printed pictures of child

pornography are not only kept near the computer, but in hidden areas that are only known to the child pornographer to keep other individuals from discovering the illegal material.

23. Affiant states that computer technology can be mobile in the form of laptop computers, removable diskettes, removable hard drives, and via remote or wireless access. Therefore, evidence, contraband, instrumentalities, or fruits of crime can be located virtually anywhere within or outside the residence or vehicle.

PROBABLE CAUSE

24. On or about April 3, 2014, Task Force Officer (TFO) Jeremy Allman received complaints from the National Center for Missing and Exploited Children (NCMEC). Two of the complaints were assigned complaint numbers 2391795 and 2376219. The complaints were filed by Google. The graphic files produced by Google in all of the below NCMEC complaints were viewed by a Google employee prior to filing the complaint and submitting the files to NCMEC.

25. The following information was provided by Google related to NCMEC complaint number 2391795:

a. On March 10, 2014, at 3:10:23 Universal Coordinate Time (UTC) from IP address 107.221.94.10, Google user koolone66@gmail.com, uploaded a picture to <https://picasaweb.google.com/103143801975274613821>. Google provided the picture in the NCMEC complaint. Affiant reviewed the picture and found it depicted two prepubescent females standing in a wooded area. One female was wearing a blue shirt and purple pants. Her pants and undergarments were pulled down to her mid-thighs clearly exposing her vagina. Her shirt was pulled up to the top of her stomach exposing her stomach area. The second female was

wearing panties and some form of shirt or top while holding a yellow cloth close to her face using both hands. The second female's panties were pulled down to her mid-thighs clearly exposing her vagina. Her top was pulled up exposing her stomach area. Lying on the ground behind them was what appeared to be a pink blanket.

b. According to the information provided by Google to NCMEC, the Google account koolone66@gmail.com is a verified account and had the secondary email address of caseycoldiron718@yahoo.com. The last log in attempt was on March 12, 2014, from IP address 107.221.94.10. The name on the account is "Lacy Truelove". The account registration date was January 31, 2014, at 15:16:53 UTC from IP address 107.221.94.10.

c. According to information provided by Google to NCMEC as reported within the NCMEC complaints, koolone66@gmail.com's Google+ account contained "one additional child sexual abuse image, as well as other images of nude children or children in sexually explicit poses." In addition to uploading the images to the Google+ account, the user "was observed posting some of these images to his Google+ Circles. The user also appeared to be posting and commenting on Google+ in regards to the trading of child sexual abuse images." Furthermore, the "account was also posting and commenting on the Google+ profiles of young girls." Google further reported that the "user also appear[ed] to be engaging in Google Hangouts with young girls." Google reported that the user of koolone66@gmail.com provided a date of birth to YouTube of June 19, 1980. And on this account "[p]rivate messages were observed in the YouTube account where the user appears to be discussing a sexual interest in young girls."

26. The following information was provided by Google related to NCMEC complaint number 2376219:

a. On March 10, 2014, at 3:51:20 UTC from IP address 107.221.94.10, koolone66@gmail.com uploaded an image to <https://picasaweb.google.com/103143801975274613821>. Affiant reviewed the image and found it depicted a prepubescent female lying on a bed. The child's entire body and face can be seen in the picture. The female was wearing a dark colored top and no clothing on the bottom half of her body. The child's shirt was pulled up just above her belly button. Her legs were spread apart clearly exposing her vagina and buttocks. One of the child's legs was bent with the knee facing upwards and her foot flat on the bed while her heel was close to her buttocks. Her second leg was lying on the bed with her knee bent pointing towards her elbow. The picture was taken as if the person taking the photograph was between her legs focusing of the child's genitals.

b. On March 10, 2014, at 3:43:53 UTC from IP address 107.221.94.10, koolone66@gmail.com uploaded an image to <https://picasaweb.google.com/103143801975274613821>. Affiant reviewed the image and found it depicted a prepubescent female lying on the floor. The child was wearing a shirt and skirt. Her legs were bent so her knees were facing up, her feet flat on the floor, and her legs were spread apart. The front of the skirt was pulled up above her pelvic region. The child was not wearing panties. The child's vagina and buttocks was clearly visible and appeared to be the focus of the photograph. The photograph appeared to be taken by someone positioned between her legs angling the camera downward.

c. Google provided a third image that was uploaded from Google account koolone66@gmail.com. Google did not provide any information related to the date and time the picture was uploaded. Affiant reviewed the picture and found it to be consistent with the picture in NCMEC complaint 2391795.

27. On or about May 27, 2014, Task Force Officer (TFO) Jeremy Allman received NCMEC complaint 2479045. The complaint was filed by Google. The following information was provided by Google related to NCMEC complaint number 2479045:

a. On May 14, 2014, between 12:00:02 and 12:00:59 UTC from IP address 107.221.94.10, Google user doll08693@gmail.com, uploaded two pictures to their Google account. Google provided the picture in the NCMEC complaint. According to Google, they reviewed the pictures prior to filing the complaint. Affiant reviewed the first picture and found it depicting one infant female lying down. The infant was unclothed with her legs spread apart and one hand on her belly. Located close to the infant's vagina was a male's penis. The infant had white liquid substance on her vagina and lower belly. The infant's vagina was clearly visible in the picture. Affiant reviewed the second picture and found it depicting a prepubescent female lying down and an adult male between her legs. The female was nude from the waist down and had her shirt pulled up to her neck area. The child's head was raised looking down towards her vaginal area. Between the child's legs was an adult male partly clothed. The male was wearing a watch and shirt. The male was not wearing any clothing from the waist down. The male was holding his erect penis with his hand while penetrating the child's vagina.

b. The Google account doll08693@gmail.com is a verified account and had the secondary email address of caseycoldiron718@yahoo.com. The account registration date was May 11, 2014, at 8:25:54 UTC from IP address 107.221.94.10.

28. On April 9, 2014, Affiant conducted a search for IP address 107.221.94.10 on the American Registry for Internet Numbers (ARIN). As stated above, both Google user

koolone66@gmail.com and doll08693@gmail.com used IP address 107.221.94.10. The Internet Service Provider (ISP) for IP address 107.221.94.10 was owned by AT&T Internet Services.

29. On May 12, 2014, an Administrative Subpoena was served on AT&T Internet Services. The subpoena requested subscriber information related to the use of IP address 107.221.94.10 on 3/10/2014 at 3:43 and 3:51 UTC.

30. On or about June 8, 2014, AT&T Internet Services responded to an Administrative Subpoena requesting subscriber information related to IP address 107.221.94.10 on March 10, 2014, at 3:43 UTC and 3:51 UTC. AT&T records showed that IP address 107.221.94.10 was assigned to address 839 15th Street, Cleveland, Tennessee under the account of Larry Oliver on November 1, 2013. According to the subpoena return provided by AT&T, the customer account was a U-verse account and included the explanation, "AT&T U-Verse internet access accounts do not have traditional session records with a standard log on/log off format. U-Verse customers have a unique IP directly provisioned to the account." Furthermore, on January 14, 2015, Affiant contacted AT&T National Court Order Compliance via telephone and made contact with a representative. The representative explained to the Affiant that after they received the subpoena request they processed the request for the requested date and times. According to the AT&T representative, the IP addressed was assigned to 839 15th Street, Cleveland, Tennessee on November 1, 2013, and was continuously assigned to the location through March 10, 2014.

31. Affiant searched the Tennessee Sex Offender Registry for "Oliver." The search resulted in locating a Kenneth Ray Oliver, date of birth June 20, 1963, white male, address 839 15th

Street, Cleveland, Tennessee. Kenneth Ray Oliver's sex offender status showed active with a violent classification.

32. Affiant received information from Detective (Det.) Shaunda Efaw of the Bradley County Sheriff's Office as it related to Kenneth Ray Oliver's sex offender registration. Kenneth Ray Oliver complied with his quarterly reporting on March 10, 2014. During the reporting, Oliver confirmed his contact number was 423-331-3972, and he lives at 839 15th Street Northeast, Cleveland, Tennessee 37311. According to Det. Efaw's records, Oliver shares the domicile and phone number with his brother, Larry Roger Oliver.

33. On October 16, 2014, Detective Kevin White and Dewayne Scoggins with the Bradley County Sheriff's Office conducted annual sex offender checks. White and Scoggins made contact with Kenneth Oliver at 839 15th Street Northeast. Oliver told them that he lives at the residence with his brother Larry Oliver. When speaking to Oliver, Detectives White and Scoggins noticed, in plain view, a computer monitor inside the residence to the left as you enter the door.

34. On November 17, 2014, Affiant conducted surveillance at 839 15th Street Northeast. During surveillance, Affiant saw a gold colored Chevrolet bearing Tennessee license plate "272 QKP". The tag number was entered into the Tennessee Vehicle Registration database which indicated the vehicle was registered to Larry Oliver of 839 15th Street Northeast, Cleveland, Tennessee 37311. As stated above, in paragraph 5 of this affidavit, Kenneth Ray Oliver confirmed on December 10, 2014, pursuant to his sex offender reporting requirements, that he continued to reside at the Subject Premises. Affiant further states that on January 22, 2015,

affiant drove past the Subject Premises at approximately 7:30 a.m. and observed the same gold colored Chevrolet, tag 272 QKP, parked in the driveway of Subject Premises.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO RECEIVE AND/OR
DISTRIBUTE CHILD PORNOGRAPHY**

35. Based upon my training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and attempt to receive child pornography:

a. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who receive and attempt to receive child pornography may collect sexually explicit or suggestive material, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Furthermore, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals

typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and kept close by usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

e. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names' addresses' and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Those who receive or attempt to receive child pornography rarely, if ever, dispose of their sexually explicit materials, especially when it is used in the seduction of their victims, and those materials are treated as prize possessions. They also utilize the photos as keepsakes and as a means of gaining acceptance, status, trust and psychological support by exchanging, trading or selling them to other people with similar interests. Persons involved in sending or receiving child pornography tend to retain it for long periods of time. The images obtained,

traded and/or sold are prized by those individuals interested in child pornography. In addition to their "emotional" value, the images are intrinsically valuable as trading/selling material and therefore are rarely destroyed or deleted by the individual collector.

FORENSIC SEIZURE AND ANALYSIS OF COMPUTERS

36. Computer hardware, computer software, computer-related documentation, passwords, and data security devices may be important to a criminal investigation in three important respects: (1) as instrumentalities for the violations of Federal Laws enumerated herein; (2) as devices used in conjunction with the collection and storage of electronic data and records related to the alleged violations and (3) fruits of illegal activity. Search and seizure of computer hardware, software, documentation, passwords, and data security devices, either as instrumentalities of criminal activity or as storage devices for evidence thereof, is contemplated at the Subject Premises.

37. Computer hardware is described as all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes, but is not limited to, any data-processing devices (such as central processing units, memory typewriters, self-contained "laptop" or "notebooks" computers, "palm pilots," and "schedulers"); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, flashdrives, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printer, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections,

recordings equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks). Moreover, electronic storage devices, smartphones, computers such as those described above can communicate with computers and the internet through wireless means, making these storage devices mobile and can be stored outside of a residence in any storage container or outside storage location such as but not limited to outbuildings, vehicles, and trash cans. Furthermore, storage media such as micro sd cards can be as small as 32 millimeters making it possible to conceal and flashdrives are being manufactured to look like but not limited to necklaces, key chains, pens, and children toys.

38. Computer software is described as digital information which can be interpreted by a computer and any of its related components to direct the way the work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

39. Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use the computer hardware, software, or other related items.

40. Computer passwords and other data security devices are described as a string of alphanumeric characters designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password usually operates as a sort of digital key to "unlock" particular data security devices.

Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

41. Based upon my knowledge, training, and experience, searching and seizing information from computers often requires law enforcement to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

b. Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Through such expertise, child pornography can be discovered on a computer's hard drive even after those images have been deleted. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are an exacting scientific procedure designed to protect the

integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of the computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. Various types of computer technologies operate in storing or processing records, in the experience of others who have conducted law enforcement training schools and seminars, that it is common to find that specific records authorized to be seized are inextricably mixed or that without employing difficult or extremely time-consuming procedures are inseparable from other records, programs, or files (similar to a bound-volume book containing financial records, addresses, a diary, and notes, for example). The items authorized to be seized will be copied for evidence purposes.

42. In light of these concerns, you Affiant hereby request the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described.

REQUEST FOR SEALING

43. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of

the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

CONCLUSION

44. Based upon information provided in this affidavit, there is probable cause to believe that evidence of violations of Title 18 U.S.C. §§ 2252A(a)(1), 2252A(a)(2), 2252A(b)(1), and 2252A(a)(5)(B) will be found at the Subject Premises. Affiant submits that evidence, listed in Attachment A to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses, and will be found in the Subject Premises.

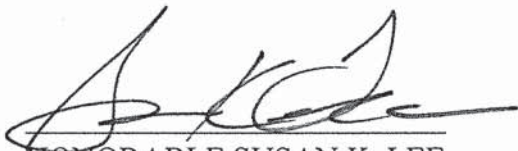
45. Finally, based on the information provided in this affidavit, there is probable cause to believe that those items set forth in Attachment A, which constitute evidence of violations against the laws of the United States, are contained within:

839 15th Street Northeast, Cleveland, Tennessee 37311.



Jeremy P. Allman, Detective
Violent Crimes Against Children Task Force
Federal Bureau of Investigation

Subscribed and sworn before me,
This 22 day of Jan., 2015



HONORABLE SUSAN K. LEE
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF ITEMS TO BE SEIZED

Affiant seeks to search for, and seize, the following materials, which constitute evidence and instrumentalities of the use of interstate or foreign commerce, to include a computer, to receive, possess or distribute images of child pornography in violation of Title 18 USC §§ 2252A(a)(1), 2252A(a)(2), 2252A(a)(5)(B), and evidence and instrumentalities of any visual depiction of child pornography that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer, in interstate or foreign commerce, including:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, §§ 2256, and any mechanism used for the receipt or storage of the same, including but not limited to:

Any computer, computer system and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
3. Any and all documents, records, e-mails, and internet history (in documentary or electronic form) pertaining to the possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code §§ 2256, or pertaining to an interest in child pornography whether transmitted or received.
4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.
5. Documents and records regarding the ownership and/or possession of the searched premises.
6. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

ATTACHMENT B1
DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as 839 15th Street Northeast, Cleveland, Tennessee 37311 is identified as follows:

The location is a mobile home located on 15th Street Northeast. When turning left on 15th Street from Overhead Bridge Road the residence is on the right-hand side of 15th Street Northeast. The residence is a blue siding home with dark skirting and three windows on the front of the residence. The roof of the residence has dark shingles. The front door is white and is accessed by a wooden porch. A chain link fence can be seen paralleling the rear of the residence. A light colored outbuilding is at the rear of the residence. A photograph of the residence is attached as Attachment B2.

B2

